AZ-ZAIDA
JURNAL ILMU MULTIDISIPLIN
Volume 1 Nomor 3 September 2025
P-ISSN: xxxx-xxxx E-ISSN: xxxx-xxxx DOI: xxxxxx

.

FRAMING PENGUNGKAPAN RISIKO SIBER: ANALISIS KONTEN LAPORAN TAHUNAN TELKOM INDONESIA

Fityan Halid[1], Usman[2]
Universitas Negeri Gorontalo
fityanhalid@gmail.com[1], usman.aman44@yahoo.com[2]

Abstract

Cyber risks have become a material issue in the governance of digital-based corporations, particularly within the telecommunications sector that manages nationally critical infrastructure. However, the maturity of cyber risk disclosure in Indonesian annual reports remains inconsistent, raising questions about how cyber risks are identified, mitigated, and framed within corporate reporting practices. This study focuses on Telkom Indonesia to examine how cyber risks are articulated in annual reports, how governance structures and mitigation mechanisms are presented, and how risk narratives are linked to regulatory compliance and business strategy. Using a case study design and qualitative content analysis, the study analyzes Telkom's 2020–2024 annual reports at the paragraph level through a deductive–inductive category framework encompassing risk identification, mitigation, governance, impacts, and strategic responses. The findings reveal a shift in disclosure from compliance-oriented narratives toward strategic framing aligned with strengthened governance and digital transformation. Network infrastructure and operational risks emerge as stable core risks, whereas privacy and data breach risks evolve from regulatory obligations into strategic risks with reputational implications. Recurring cyberattacks since 2022 indicate increasing maturity in risk identification. Mitigation is carried out through technical, operational, and organizational controls integrated with internal control systems. Telkom's cyber risk disclosure is governance-driven and framed as part of the company's digital strategy as well as a mechanism for legitimizing corporate accounting disclosures. These findings contribute to the accounting and risk disclosure literature by demonstrating how a national digital corporation constructs cyber risk as an integral component of governance and corporate strategy.

Keywords: Cyber Risk; Disclosure; Governance; Content Analysis; Corporate Reporting

AZ-ZAIDA
JURNAL ILMU MULTIDISIPLIN
Volume 1 Nomor 3 September 2025
P-ISSN: xxxx-xxxx E-ISSN: xxxx-xxxx DOI: xxxxxx

Abstrak

Risiko siber menjadi isu material dalam tata kelola perusahaan digital, khususnya pada sektor telekomunikasi yang mengelola infrastruktur kritikal nasional. Namun tingkat kematangan pengungkapan risiko siber pada laporan tahunan di Indonesia belum konsisten, sehingga memunculkan pertanyaan mengenai bagaimana risiko siber diidentifikasi, dimitigasi, dan dibingkai dalam pelaporan korporat. Penelitian ini berfokus pada Telkom Indonesia untuk menjawab bagaimana risiko siber diartikulasikan dalam laporan tahunan, bagaimana struktur tata kelola dan mitigasi ditampilkan, serta bagaimana narasi risiko dikaitkan dengan kepatuhan dan strategi bisnis. Metode yang digunakan adalah studi kasus dengan pendekatan *qualitative content analysis* terhadap laporan tahunan 2020–2024, dianalisis pada unit paragraf melalui kerangka kategori deduktif–induktif mencakup identifikasi risiko, mitigasi, tata kelola, dampak, dan strategi. Hasil penelitian menunjukkan bahwa pengungkapan risiko siber Telkom mengalami pergeseran dari narasi kepatuhan menuju framing strategis seiring penguatan tata kelola dan transformasi digital. Risiko infrastruktur dan operasional jaringan muncul sebagai core risk yang stabil, sementara risiko privasi dan kebocoran data berkembang menjadi risiko strategis dengan implikasi reputasi. Serangan siber aktif berulang sejak 2022, menunjukkan peningkatan maturitas identifikasi risiko. Mitigasi dilakukan melalui kontrol teknis, operasional, dan organisasi yang terintegrasi dengan pengendalian internal. Pengungkapan risiko siber Telkom bersifat *governance-driven* dan dibingkai sebagai bagian dari strategi digital serta mekanisme legitimasi dalam pelaporan akuntansi korporat. Temuan ini berkontribusi pada literatur akuntansi dan pengungkapan risiko dengan menunjukkan bagaimana perusahaan digital nasional mengonstruksi risiko siber sebagai bagian dari tata kelola dan strategi korporat.

Kata kunci: Risiko Siber; Pengungkapan; Tata Kelola; Analisis Konten; Pelaporan Korporat

A. PENDAHULUAN

Percepatan digitalisasi bisnis sejalan dengan transformasi ekonomi berbasis data. Kondisi ini mendorong perusahaan membangun model layanan yang bertumpu pada integrasi data, komputasi awan, dan sistem informasi berbasis jaringan. Ketergantungan tinggi pada teknologi tersebut melahirkan bentuk risiko baru yang semakin menonjol, yaitu risiko siber (*cyber risk*). Risiko ini mencakup serangan siber, kebocoran data, gangguan sistem, *ransomware*, serta penyalahgunaan data yang berpotensi menimbulkan kerugian finansial, kerusakan reputasi, gangguan operasional, hingga risiko hukum. Berbagai penelitian terdahulu menunjukkan bahwa peningkatan

digitalisasi diikuti oleh pertumbuhan eksponensial insiden kejahatan siber, terutama di sektor jasa keuangan dan perusahaan yang mengelola data pengguna dalam skala besar, termasuk sektor berbasis platform, perbankan digital, dan penyedia layanan telekomunikasi. Tren global menunjukkan bahwa digitalisasi di berbagai negara juga meningkatkan kompleksitas ancaman siber dan kebutuhan akan pengungkapan risiko yang lebih transparan (Georg-Schaffner dkk., 2021; Ramírez dkk., 2022). Amalina & Sari (2025) menunjukkan bahwa sektor perbankan di Indonesia menghadapi ancaman serius terkait keamanan siber seiring meningkatnya penggunaan layanan digital dan integrasi dengan platform teknologi keuangan. Jubaedah dkk. (2025) juga mengemukakan bahwa data dari otoritas nasional dan lembaga keamanan siber global memperlihatkan nilai kerugian ekonomi yang signifikan akibat serangan siber di sektor keuangan Indonesia. Y. P. Sari dkk. (2023) menunjukkan bahwa percepatan digitalisasi selama pandemi meningkatkan paparan risiko siber bagi organisasi, termasuk BUMN yang menjadi objek penelitian mereka. Implikasi akuntansi dan tata kelola ini mengindikasikan kebutuhan terhadap praktik pengungkapan risiko siber yang lebih komprehensif, tetapi literatur menunjukkan bahwa praktik tersebut belum berkembang secara merata.

Dari sudut pandang akuntansi dan tata kelola perusahaan (*corporate governance*), risiko siber bukan lagi sekadar persoalan teknis teknologi informasi. Risiko ini memiliki implikasi langsung terhadap kualitas informasi akuntansi, pengakuan dan pengukuran aset, serta liabilitas, penyajian dan pengungkapan dalam laporan keuangan, serta mekanisme akuntabilitas perusahaan kepada para pemangku kepentingan. Serangan siber dan kebocoran data dapat memicu penurunan pendapatan, peningkatan beban remediasi, pembentukan provisi atas potensi gugatan (misalnya berdasarkan PSAK 57), hingga penurunan nilai aset tak berwujud dan aset teknologi (PSAK 19 dan PSAK 48). Simanjuntak dkk. (2025) menekankan bahwa keamanan sistem informasi akuntansi merupakan prasyarat penting bagi keandalan laporan keuangan dan akuntabilitas perusahaan, gangguan terhadap sistem informasi akuntansi akibat serangan siber dapat mengancam kualitas informasi yang dihasilkan. Ditinjau dari sudut tata kelola, **pengungkapan risiko siber (*cybersecurity disclosure*)** telah berkembang menjadi instrumen akuntabilitas yang memengaruhi persepsi pemangku kepentingan. Elsayed dkk. (2024) menunjukkan bahwa tingkat pengungkapan keamanan siber berhubungan positif dengan kinerja bank, sementara kehadiran struktur governance seperti *Chief Risk Officer* dan komite TI memperkuat hubungan tersebut. Temuan ini mengindikasikan bahwa *cyber risk disclosure* tidak hanya berfungsi informatif, tetapi juga merupakan **mekanisme *governance*** untuk mengurangi asimetri informasi. Penelitian lain mengaitkan pengungkapan risiko siber dengan **nilai perusahaan** (Jameel dkk., 2025), dan dengan **biaya audit**, di mana ekspansi narasi risiko

meningkatkan persepsi risiko auditor yang berujung pada kenaikan *audit fees* (Susanto & Soepriyanto, 2024). Dengan demikian, *cyber disclosure* memiliki konsekuensi ekonomi yang material, bukan sekadar kepatuhan normatif. Sejalan dengan pendekatan *risk communication* dalam literatur akuntansi, kualitas pengungkapan risiko tidak hanya bergantung pada detail informasi, tetapi juga bagaimana perusahaan membingkai risiko tersebut dalam konteks tata kelola dan strategi bisnis. Penelitian lain juga menunjukkan bahwa kualitas pengungkapan keamanan siber memiliki implikasi langsung terhadap kualitas pelaporan keuangan dan persepsi pasar (Amin Elnagar dkk., 2024), terutama pada pasar berkembang seperti Amerika Latin yang masih mengandalkan pola *voluntary disclosure* (Ramírez dkk., 2022).

Meskipun signifikansinya tinggi, literatur menunjukkan bahwa praktik pengungkapan risiko siber di negara berkembang, termasuk Indonesia, masih bersifat ***voluntary*** dan tidak terstandar. Sistem pelaporan perusahaan publik belum menyediakan pedoman eksplisit mengenai bagaimana risiko siber harus didefinisikan, dikategorikan, atau dikaitkan dengan tata kelola (L. Sari dkk., 2024). Kajian empiris yang ada umumnya berfokus pada determinan kuantitatif seperti karakteristik dewan (Amalina & Sari, 2025), struktur kepemilikan (Jubaedah dkk., 2025), atau ukuran perusahaan (Sofiani dkk., 2024), dengan objek dominan pada sektor perbankan. Pendekatan ini menjelaskan "seberapa banyak" risiko siber diungkap, namun tidak menjelaskan **bagaimana perusahaan menyusun narasi risiko siber, menempatkannya dalam kerangka *governance*, dan mengaitkannya dengan strategi bisnis**. Kondisi ini sejalan dengan temuan internasional bahwa standar pengungkapan risiko siber masih bervariasi dan sebagian besar bersifat *voluntary*, bahkan pada pasar modal yang lebih maju (Georg-Schaffner dkk., 2021; Singh, 2025).

Kesenjangan penelitian menjadi semakin penting pada sektor telekomunikasi, yang merupakan **infrastruktur digital utama**. Berbeda dari bank yang mengelola data keuangan, perusahaan telekomunikasi menangani jaringan, komunikasi, data pelanggan, serta platform layanan yang menjadi fondasi aktivitas ekonomi nasional. Perusahaan seperti PT Telkom Indonesia memiliki profil risiko operasional dan reputasi yang tinggi, namun masih terbatas penelitian yang mendalami bagaimana Telkom mengonstruksi pengungkapan risiko siber dalam laporan tahunan. Padahal, sebagai entitas strategis yang menjalankan transformasi digital 2020-2024, Telkom menghadapi tekanan tata kelola dan kebutuhan legitimasi publik yang unik, termasuk ekspektasi transparansi terkait kerentanan sistem, mekanisme mitigasi, serta integrasi risiko siber dalam *governance*. Sebagai BUMN sekaligus entitas yang terdaftar di *New York Stock Exchange* (NYSE), Telkom berada dalam tekanan institusional ganda yang menjadikannya kasus penting untuk memahami praktik pengungkapan risiko siber di negara berkembang. Sejalan dengan observasi Ramírez dkk. (2022) bahwa sektor-

sektor berperan kritis, termasuk energi dan keuangan, menunjukkan pola kerentanan dan tuntutan pengungkapan yang lebih tinggi, sebuah kondisi yang relevan juga bagi sektor telekomunikasi.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk **menganalisis** bagaimana Telkom mengidentifikasi, memitigasi, dan membingkai risiko siber dalam laporan tahunan 2020–2024, serta bagaimana *framing* tersebut terintegrasi dengan tata kelola risiko dan strategi transformasi digital perusahaan. Fokus penelitian bukan pada kuantitas *disclosure*, tetapi pada **struktur naratif, kategorisasi risiko, dan posisi risiko siber dalam kerangka tata kelola perusahaan**, guna memahami bagaimana risiko ini dikomunikasikan kepada pemangku kepentingan. Dengan demikian, penelitian ini memberikan kontribusi terhadap literatur akuntansi dengan menggeser perspektif dari determinan numerik menuju **pemaknaan risiko siber sebagai bagian dari akuntabilitas korporat**, serta memperluas diskursus pengungkapan risiko dari sektor perbankan ke sektor telekomunikasi sebagai infrastruktur digital nasional. Pendekatan ini sejalan dengan penelitian yang menekankan pentingnya transparansi risiko siber dalam memenuhi ekspektasi *stakeholder* (Singh, 2025).

B. METODE

Penelitian ini menggunakan **desain studi kasus** dengan objek PT Telkom Indonesia untuk memahami bagaimana perusahaan membingkai risiko siber dalam konteks tata kelola organisasi. Studi kasus digunakan untuk menyelidiki fenomena kontemporer dalam konteks dunia nyata, terutama ketika batas antara fenomena dan konteks tidak jelas, dan sangat sesuai untuk menjawab pertanyaan "*how*" (Yin, 2018). Sumber data utama adalah **Laporan Tahunan Telkom 2020–2024**, yang dikumpulkan dengan mengunduh dokumen resmi dari situs perusahaan dan kemudian mengekstraksi seluruh paragraf terkait risiko digital. Analisis dilakukan menggunakan *qualitative content analysis*, yaitu teknik interpretatif yang menafsirkan teks melalui proses inferensi yang mengaitkan isi pesan dengan konteks sosial atau organisasional yang melingkupinya, sesuai prinsip *semantic validity* (Krippendorff, 2022). Pendekatan ini digunakan bukan untuk menghitung frekuensi istilah, tetapi untuk mengidentifikasi cara risiko dipresentasikan, diprioritaskan, dan diposisikan dalam kerangka tata kelola perusahaan. Setiap laporan diimpor ke MaxQDA, dipisah ke unit paragraf, dan diseleksi menggunakan kombinasi pencarian kata kunci serta pembacaan manual untuk mengidentifikasi paragraf relevan. Unit analisis dalam penelitian ini adalah paragraf, karena paragraf merepresentasikan satuan makna yang utuh dalam laporan tahunan sehingga sesuai untuk analisis isi kualitatif. Penggunaan MaxQDA juga memungkinkan dokumentasi audit *trail*, konsistensi *coding*, dan penelusuran ulang keputusan analitis selama proses penelitian.

Kerangka kategori dikembangkan melalui kombinasi pendekatan deduktif dan induktif (*combined deductive–inductive category development*) sebagaimana dijelaskan oleh Kuckartz & Rädiker (2023). Kerangka deduktif dibangun dari standar manajemen risiko (COSO, 2017; ISO 31000, 2018), kerangka risiko siber (NIST, 2018), serta prinsip tata kelola risiko korporat (OECD, 2014). Untuk kategori Strategi & Transformasi Digital, penelitian ini merujuk pada kerangka konseptual Gong & Ribiere (2021) yang memandang transformasi digital sebagai proses perubahan fundamental yang didorong oleh pemanfaatan inovatif teknologi digital dan kapabilitas organisasi untuk menciptakan nilai baru. Integrasi berbagai kerangka ini diperlukan karena pengungkapan risiko siber Telkom tidak hanya menggambarkan ancaman teknis, tetapi juga mencakup strategi mitigasi, struktur tata kelola, dampak risiko, serta respon strategis organisasi digital.

Proses *coding* dilakukan secara **iteratif**, dimulai dengan penerapan kategori deduktif, kemudian diperluas secara **induktif** sesuai pola naratif yang ditemukan dalam laporan. *Coding* juga dilakukan **lintas tahun** untuk menjaga konsistensi, mengevaluasi kejenuhan subkategori, dan mengidentifikasi perubahan *framing* risiko siber. Dengan demikian, kerangka kategori yang dihasilkan tidak hanya *grounded* pada teori risiko dan *governance*, tetapi juga secara langsung merefleksikan cara organisasi membingkai risiko siber dalam dokumentasi resmi mereka. Konsistensi interpretasi dijaga melalui penggunaan memo analitik dan *constant comparison* lintas tahun selama proses *coding*.

C. HASIL DAN PEMBAHASAN

Analisis pengungkapan risiko siber PT Telkom Indonesia dalam laporan tahunan 2020–2024 menunjukkan adanya evolusi penting dalam cara perusahaan mengidentifikasi, memitigasi, dan membingkai risiko siber, yang semakin terintegrasi dengan tata kelola risiko dan strategi transformasi digital perusahaan. Dengan menggunakan pendekatan *qualitative content analysis*, temuan-temuan ini diperoleh dari kategori dan subkategori yang telah disusun secara sistematis, kemudian ditafsirkan melalui dialog dengan literatur primer terkini dalam bidang akuntansi, tata kelola, dan keamanan siber. Pendekatan naratif ini sejalan dengan perkembangan literatur global yang menekankan pentingnya analisis struktur dan kualitas pengungkapan risiko siber, bukan hanya kuantitas (Ramírez dkk., 2022).

Subkategori Risiko	Tahun Kemunculan	Pola Umum
Infrastruktur & Operasional	2020–2024	Risiko paling stabil; berkaitan dengan jaringan, satelit, dan layanan inti

.

Privasi & Kebocoran Data	2020, 2023, 2024	Bergeser dari *compliance* ke *strategic risk*
Serangan Siber Aktif	2022–2024	Ancaman eksternal berulang (*brute force*, *DDoS*, *DC threats*)
Regulasi & Kepatuhan Digital	2020–2024	Risiko kepatuhan stabil, dipengaruhi *dual-regulatory regime*

Tabel C1. Ringkasan Identifikasi Risiko Siber Telkom 2020–2024

Pengungkapan risiko Telkom dalam lima tahun terakhir menegaskan bahwa risiko infrastruktur dan operasional jaringan merupakan risiko inti yang konsisten. Kutipan seperti *"kegagalan dalam keberlanjutan operasi jaringan, sistem utama, gateway"* serta *"keterbatasan masa operasional satelit, kerusakan atau penundaan peluncuran"* menunjukkan bahwa risiko-risiko ini tidak mengalami perubahan berarti dari waktu ke waktu. Konsistensi ini memperlihatkan bahwa Telkom menghadapi *core risk* yang melekat pada model bisnis telekomunikasi. Temuan ini sejalan dengan Y. P. Sari dkk. (2023), yang menekankan bahwa SOE membutuhkan tata kelola risiko yang kuat untuk menjaga stabilitas operasional di tengah percepatan digitalisasi. Dalam konteks Telkom, risiko ini bahkan memiliki bobot strategis yang lebih besar karena perannya sebagai penyedia infrastruktur digital nasional. Temuan ini konsisten dengan analisis Georg-Schaffner dkk. (2021) yang menunjukkan bahwa beberapa kategori risiko cenderung bersifat generik dan berulang dari tahun ke tahun.

Di luar risiko operasional, perkembangan yang paling menonjol adalah perubahan cara Telkom membingkai risiko privasi dan kebocoran data. Pada dua tahun awal, isu privasi diposisikan sebagai kewajiban regulatif, tetapi sejak 2023 Telkom mulai menegaskan bahwa pencurian data dan serangan siber dapat menimbulkan ancaman reputasi dan gangguan operasional yang serius, sebagaimana tercermin dalam kutipan: *"Ancaman seperti serangan cyber dan pencurian data dapat merusak reputasi perusahaan dan mengganggu operasional."* Perubahan naratif ini memperlihatkan bahwa risiko privasi tidak lagi diperlakukan sebagai risiko kepatuhan, tetapi telah bertransformasi menjadi risiko strategis. Temuan analisis ini sejalan dengan ulasan Amani dkk. (2025), yang menunjukkan bahwa isu privasi dan data *breach* memiliki dampak luas terhadap legitimasi, persepsi publik, serta tekanan institusional yang menjadikannya bagian dari risiko strategis dalam konteks modern. Pola serupa juga diidentifikasi oleh Jubaedah dkk. (2025), yang menunjukkan bahwa data breach menimbulkan kekhawatiran signifikan di pasar dan berimplikasi pada kepercayaan pemangku kepentingan. Simanjuntak dkk. (2025) turut menekankan bahwa gangguan terhadap integritas data dapat mengancam keandalan sistem informasi akuntansi (AIS), sehingga risiko privasi memiliki implikasi langsung terhadap tata kelola pelaporan keuangan. Amin Elnagar dkk. (2024) menunjukkan

bahwa risiko siber berdampak pada integritas dan keandalan data akuntansi, sehingga memengaruhi kualitas pelaporan keuangan dan persepsi investor.

Kesadaran atas serangan siber aktif semakin menonjol sejak 2022. Risiko seperti *"brute force attack, DDoS attack, dan threats to Data Center"* tidak hanya muncul sekali, tetapi berulang hingga 2024, memperlihatkan pola *persistent threat*. Konsistensi klasifikasi serangan menurut Kuckartz & Rädiker (2023) menunjukkan bahwa Telkom telah mencapai *risk identification maturity*, di mana organisasi mampu mengidentifikasi ancaman dengan stabil melalui kerangka analitis yang terstandarisasi. Pola ini juga didukung oleh literatur global (Elsayed dkk., 2024), yang menegaskan bahwa perusahaan digital akan menghadapi pola ancaman yang berulang dan membutuhkan mekanisme mitigasi yang konsisten. Pola ancaman berulang di Telkom sejalan dengan temuan Gao dkk. (2020) bahwa risiko operasional dan kebocoran data merupakan kategori yang paling konsisten diungkapkan perusahaan publik AS dari tahun ke tahun.

Selain itu, regulasi merupakan salah satu risiko yang paling stabil sepanjang periode penelitian. Penegasan Telkom bahwa *"Telkom diwajibkan menerapkan manajemen risiko yang memenuhi Sarbanes-Oxley Act"* menunjukkan bahwa risiko kepatuhan menjadi bagian fundamental dari operasi korporat. Keberadaan dual regulatory regime antara kewajiban sebagai BUMN dan perusahaan yang terdaftar di NYSE meningkatkan intensitas pengungkapan risiko, selaras dengan temuan Gao dkk. (2020) bahwa perusahaan yang berada di bawah kewajiban pelaporan multi-jurisdiksi cenderung mengungkap risiko secara lebih intensif. Gao dkk. (2020) menemukan bahwa risiko regulasi merupakan salah satu dari enam kategori utama pengungkapan risiko siber yang digunakan perusahaan, di mana rincian mengenai risiko ini umumnya muncul pada Item 1 (*Business*) dalam laporan tahunan. Dengan demikian, risiko regulasi merupakan dimensi struktural yang memengaruhi bagaimana Telkom membingkai risiko siber.

Subkategori	Tahun Kemunculan	Pola Umum
SOC/SIEM & Security Tools	2020–2024	Mitigasi teknis stabil dan berulang
BCP/DRP & Continuity	2020–2024	Kapabilitas continuity sangat konsisten
Sistem & Standar	2020–2024	ISO, IMS, SMK3, Sidomo; mendukung governance
Fraud & Data Governance	2020–2024	Integrasi penuh dalam ICOFR
Struktur Organisasi Risiko	2020–2024	Penguatan signifikan 2020–2021, stabil setelahnya
Komite Pengawasan Risiko	2020–2024	Peran komite meningkat, khususnya 2024

.

Risk Appetite & ERM Integration	2020–2024	ERM terinstitusi dalam perencanaan
Sistem Kontrol Internal	2020–2024	Pengendalian internal konsisten dan matang
Kepatuhan Regulatif	2020–2024	SOX, Permen BUMN, OJK: tekanan regulasi berlapis

Tabel C2: Ringkasan Mitigasi & Tata Kelola Risiko Siber 2020-2024

Dari sisi mitigasi, Telkom menerapkan pendekatan *multi-layer* yang mencakup mekanisme teknis, operasional, organisasi, hingga finansial. Di ranah teknis, sistem *Security Operation Center* (SOC) dan *Security Information and Event Management* (SIEM) dijalankan secara konsisten melalui *vulnerability assessment*, *penetration testing*, *real-time monitoring*, dan analisis historis, yang seluruhnya direplikasi dari tahun ke tahun. Aktivitas mitigasi yang berulang dan terdokumentasi ini menunjukkan bahwa Telkom telah berada pada tingkat *operational maturity* dan membangun *cyber resilience capability* yang kuat (L. Sari dkk., 2025; Simanjuntak dkk., 2025). Pada level operasional, *Business Continuity Planning* (BCP) menjadi salah satu kapabilitas mitigasi paling stabil, ditandai dengan pembaruan BCP, *business impact analysis*, *risk assessment*, dan *testing* berkala. Pola ini sejalan dengan temuan Sofiani dkk. (2024) yang menegaskan bahwa perusahaan dengan ketergantungan digital dan ukuran besar cenderung meningkatkan kualitas pengungkapan risiko, termasuk aspek-aspek yang terkait dengan keberlanjutan operasional. Studi indeks pengungkapan siber juga menunjukkan bahwa perusahaan dengan struktur mitigasi *multi-layer* cenderung memiliki kualitas pengungkapan yang lebih tinggi (Ramírez dkk., 2022).

Di luar mitigasi teknis dan operasional, Telkom secara konsisten menggunakan mekanisme organisasi seperti Sidomo, SMK3 Online, *i-Library*, ICCA, dan EITA untuk menjaga integritas dokumentasi dan kebijakan. Hal ini menunjukkan bahwa manajemen risiko tidak hanya ditunjukkan melalui aspek teknis, tetapi juga melalui transparansi dan kebijakan organisasi, sejalan dengan pandangan Jameel dkk. (2025) bahwa *cybersecurity disclosure* merupakan sinyal *governance* yang meningkatkan nilai perusahaan. Kompleksitas mitigasi meningkat dengan integrasi penuh *fraud governance* ke dalam kerangka *Internal Control Over Financial Reporting* (ICOFR), termasuk ELC, TLC, RCM, dan CSA. Temuan ini memperlihatkan integrasi kuat antara keamanan digital dengan sistem pengendalian internal, mendukung pandangan bahwa pengendalian internal modern tidak dapat dipisahkan dari keamanan informasi (Simanjuntak dkk., 2025).

Dari perspektif tata kelola risiko, Telkom menegaskan komitmen institusional melalui perubahan struktur organisasi risiko yang lebih kuat dan peningkatan jumlah pegawai dari 9 menjadi 26–28 orang. Perubahan ini

mencerminkan proses institusionalisasi tata kelola risiko, sesuai dengan kerangka *risk governance institutionalization* (L. Sari dkk., 2025). Komite risiko seperti Komite Audit, KEMPR, dan Komite Tata Kelola Terintegrasi memiliki peran signifikan dalam mengawasi risiko dan memberikan legitimasi terhadap pengungkapan risiko siber. Hasil analisis ini mendukung argumen Elsayed dkk. (2024) bahwa struktur governance yang kuat berkontribusi pada kedalaman pengungkapan risiko. Posisi Telkom sebagai perusahaan telekomunikasi berbasis teknologi tinggi selaras dengan temuan Singh (2025), bahwa perusahaan di sektor *knowledge-intensive* cenderung mengungkap risiko siber lebih ekstensif.

Integrasi *Enterprise Risk Management* (ERM) ke dalam proses perencanaan bisnis terlihat dari penggunaan *risk factor* dalam penyusunan *Corporate Strategic Scenario* (CSS) dan Rencana Kerja Anggaran Perseroan (RKAP), serta pembaruan *risk appetite*, *risk universe*, dan ERM *roadmap* setiap tahun. Integrasi *risk factor* dalam perencanaan bisnis Telkom sejalan dengan temuan Jubaedah dkk. (2025) bahwa pengungkapan risiko, termasuk risiko siber, merupakan bagian penting dalam memenuhi kebutuhan informasi strategis para pemangku kepentingan, khususnya pemegang saham.

Secara keseluruhan, narasi pengungkapan Telkom menunjukkan bahwa risiko siber diperlakukan sebagai risiko bisnis yang memiliki implikasi lintas-operasional, finansial, dan reputasi. Pernyataan eksplisit bahwa risiko dapat memengaruhi *"bisnis, kondisi keuangan, hasil operasi, dan prospek usaha"* menunjukkan bahwa risiko siber melampaui risiko teknis dan telah diperlakukan sebagai *value-at-risk*, sejalan dengan pandangan (Jameel dkk., 2025).

Jika dilihat secara longitudinal, pola pengungkapan risiko siber Telkom menunjukkan bahwa perusahaan tidak bersifat reaktif terhadap insiden atau gangguan tertentu, tetapi merespons tekanan regulatif, perkembangan infrastruktur digital nasional, serta kebutuhan legitimasi di tengah transformasi digital. Karakter ini konsisten dengan konsep *governance-driven disclosure*, yakni praktik pengungkapan yang dibentuk oleh tuntutan institusional, struktur tata kelola, dan kewajiban akuntabilitas publik (Elsayed dkk., 2024). Dalam konteks Telkom, dorongan *dual-regulatory regime* (BUMN dan NYSE), intensifikasi standar keamanan digital, serta penguatan peran komite pengawasan terlihat menjadi faktor utama yang memengaruhi kedalaman dan stabilitas pengungkapan risiko. Temuan ini konsisten dengan pola pengungkapan yang diperhatikan Ramírez dkk. (2022) di Amerika Latin. Pada konteks Mesir, Amin Elnagar dkk. (2024) menemukan bahwa pengungkapan risiko siber meningkatkan kepercayaan investor dan nilai pasar.

Temuan ini mengindikasikan bahwa Telkom berhasil membangun kerangka manajemen risiko yang matang: identifikasi risiko berkembang dari risiko operasional menuju risiko reputasional dan regulatif; mitigasi

dijalankan melalui pendekatan *multi-layer* yang mencakup kontrol teknis, operasional, organisasi, dan finansial; *framing* risiko bertransformasi dari ancaman teknologi menjadi komponen strategis dalam agenda transformasi digital; dan tata kelola risiko terintegrasi dalam perencanaan bisnis, struktur organisasi, dan proses ERM. Konsistensi ini tidak hanya menjawab pertanyaan penelitian, tetapi sekaligus memperlihatkan bahwa pengungkapan risiko memiliki fungsi strategis sebagai mekanisme komunikasi risiko, penjamin legitimasi, serta alat pembentukan persepsi pemangku kepentingan terhadap kesiapan digital perusahaan. Hasil analisis ini sejalan dengan literatur yang menunjukkan bahwa karakteristik perusahaan dan tekanan pasar berperan dalam membentuk tingkat pengungkapan risiko siber (Singh, 2025).

Dari perspektif akademik, pola ini mendukung argumen bahwa organisasi dengan tingkat digitalisasi tinggi cenderung membangun narasi risiko yang bersifat institusional, bukan insidental (Simanjuntak dkk., 2025). Dengan demikian, pengungkapan Telkom tidak sekadar menggambarkan kondisi risiko, tetapi juga berfungsi sebagai representasi tata kelola digital dan kapabilitas ketahanan siber perusahaan. Hal ini memperkuat kontribusi teoretis penelitian, yaitu menunjukkan bagaimana perusahaan teknologi nasional mengonstruksi risiko siber sebagai bagian dari strategi *governance* dan transformasi digital secara simultan.

D. KESIMPULAN

Penelitian ini menganalisis pengungkapan risiko siber PT Telkom Indonesia dalam laporan tahunan 2020–2024 melalui pendekatan *qualitative content analysis*. Temuan menunjukkan bahwa Telkom mengembangkan pemahaman dan framing risiko siber secara semakin komprehensif dan strategis. Risiko yang awalnya berfokus pada aspek operasional dan infrastruktur secara bertahap bergeser menuju risiko reputasional, privasi data, serta kepatuhan regulatif. Proses ini mencerminkan peningkatan kedewasaan organisasi dalam mengenali risiko siber sebagai bagian integral dari transformasi digital.

Dari sisi mitigasi, Telkom menerapkan pendekatan *multi-layer* yang meliputi mekanisme teknis, operasional, institusional, dan finansial. Konsistensi aktivitas seperti SOC/SIEM, *vulnerability assessment*, *Business Coontinuity Plan* (BCP), *Disaster Recovery Plan* (DRP), integrasi standar *Integrated Management System* (IMS), serta penguatan pengendalian internal melalui ICOFR menunjukkan bahwa perusahaan tidak hanya berupaya mencegah insiden, tetapi juga membangun ketahanan (*cyber resilience*) jangka panjang. Sementara itu, tata kelola risiko menjadi fondasi yang memungkinkan transformasi ini berjalan secara sistematis. Penguatan struktur organisasi risiko, keterlibatan komite pengawasan, serta integrasi ERM dalam perencanaan bisnis membuktikan bahwa pengungkapan risiko

Telkom bersifat *governance-driven* dan bukan reaktif terhadap insiden tertentu.

Secara keseluruhan, penelitian ini menyimpulkan bahwa Telkom membingkai risiko siber sebagai elemen strategis dalam transformasi digital, bukan sekadar ancaman teknologi. *Framing* ini menciptakan narasi korporat yang menekankan kesiapan, legitimasi tata kelola, serta komitmen terhadap keberlanjutan bisnis. Dengan demikian, pengungkapan risiko siber dalam dokumen perusahaan tidak hanya berfungsi sebagai pelaporan kepatuhan, tetapi juga sebagai instrumen komunikasi strategis kepada pemangku kepentingan. Penelitian ini berkontribusi pada literatur akuntansi dan tata kelola risiko dengan menunjukkan bagaimana *framing* risiko siber dibentuk oleh struktur governance dan agenda transformasi digital.

Penelitian ini membuka peluang riset lanjutan, seperti analisis komparatif antar BUMN atau perusahaan telekomunikasi regional, kajian hubungan antara pengungkapan risiko dan kinerja keuangan, serta eksplorasi lebih lanjut mengenai integrasi risiko siber dengan sistem akuntansi manajemen dan tata kelola data. Studi mendalam mengenai bagaimana budaya organisasi memengaruhi cara risiko siber dipersepsikan juga menjadi arah penelitian yang relevan di masa mendatang. Temuan ini relevan bagi regulator dan pemangku kepentingan dalam memahami bagaimana perusahaan publik menavigasi tuntutan tata kelola risiko siber yang semakin kompleks.

Penulis menyampaikan penghargaan kepada seluruh pihak yang telah berkontribusi dalam proses penelitian ini, termasuk penyedia data, rekan sejawat yang memberikan masukan akademik, serta lembaga yang mendukung kegiatan penelitian ini.

.

DAFTAR PUSTAKA

Amalina, N., & Sari, V. F. (2025). Karakteristik Dewan Dan Cybersecurity Disclosure (CSD) Pada Perusahaan Perbankan Indonesia. *E-Jurnal Akuntansi*, *35(10)*, 2063–2077. https://doi.org/10.24843/EJA.2025.v35.i10.p03

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Incidents Disclosure: A Literature Review*. *Accounting Perspectives*, *24*(3), 605–667. https://doi.org/10.1111/1911-3838.12411

Amin Elnagar, S. M., Said, A., Ahmed, A. A., Mohamed, M., & Basiouny, M. (2024). Citation: Marwa Mohamed Maher Basiouny et al. (2024) The Impact Of Cybersecurity Risk Disclosure On The Quality Of Financial Reporting And Market Value. Evidence From Egyptian Stock Market. *Theory and Practice*, *2024*(5), 2504–2516. https://doi.org/10.53555/kuey.v30i5.3310

COSO. (2017). *Committee of Sponsoring Organizations of the Treadway Commission Board Members PwC-Author Principal Contributors*. https://www.coso.org/enterprise-risk-management

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, *10*(1). https://doi.org/10.1186/s43093-024-00402-9

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

Georg-Schaffner, L., Strasbourg, E. M., School, B., Behnam, E., & Pallud, J. (2021). Cyber risk disclosure: How transparent are CAC40 Companies in their Annual Reports? *submitted to Association of Information Management Conference 2021*.

Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, *102*. https://doi.org/10.1016/j.technovation.2020.102217

ISO 31000. (2018). *Risk management-Guidelines INTERNATIONAL STANDARD ISO 31000 ISO 31000:2018(E)*. www.iso.org

Jameel, A. H., Khalaf, A. J., Saleh, A. F., Sadaa, A. M., Hindi, W. K., Abdulateef, D. A., & Mahdi, A. S. (2025). Corporate Value at Risk: Why We Should Care About Climate (IFRS S2) and Cybersecurity Risks? *International Journal of Sustainable Development and Planning*, *20*(7), 3073–3083. https://doi.org/10.18280/ijsdp.200732

Jubaedah, S., Musta'in, A., Nurlisti, I., & Adam Ma
ulana, B. (2025). Cyber risk management disclosure: A stakeholder theory perspective. *Diponegoro International Journal of Business*, *7*(2), 133–146. https://doi.org/10.14710/dijb.7.2.2024.133-146

Krippendorff, K. (2022). Content Analysis: An Introduction to Its Methodology. Dalam *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, Inc. https://doi.org/10.4135/9781071878781

Kuckartz, U., & Rädiker, S. (2023). *QUALITATIVE CONTENT ANALYSIS*.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

OECD. (2014). *Risk Management and Corporate Governance* (Corporate Governance). OECD Publishing. https://doi.org/10.1787/9789264208636-en

Ramírez, M., Ariza, L. R., Miranda, M. E. G., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability (Switzerland)*, *14*(3). https://doi.org/10.3390/su14031390

Sari, L., Adam, M., Fuadah, L. L., & Yusnaini, . (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. *KnE Social Sciences*, 387–398. https://doi.org/10.18502/kss.v9i14.16113

Sari, L., Adam, M., Fuadah, L., & Yusnaini. (2025). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *TPM – Testing, Psychometrics, Methodology in Applied Psychology*, 221–240. https://tpmap.org/submission/index.php/tpm/article/view/469

Sari, Y. P., Suhardjanto, D., Probohudono, A. N., & Honggowati, S. (2023). Cyber Risk Management Disclosure of State-Owned Enterprises. *Jurnal Dinamika Akuntansi*, *15*(2), 180–190. https://doi.org/10.15294/jda.v15i2.44817

Simanjuntak, H. E., Purba, H. C., Br Ginting, J. T., Aruan, P. A., Panjaitan, R. J. N., & Darma, J. (2025). Keamanan Sistem Informasi Akuntansi dalam Era Digital: Konsep dan Implementasi. *Indo-MathEdu Intellectuals Journal*, *6*(2), 2695–2705. https://doi.org/10.54373/imeij.v6i2.2950

Singh, H. (2025). Voluntary cybersecurity risk disclosures and firms' characteristics: the moderating role of the knowledge-intensive industry. *Asian Journal of Accounting Research*, *10*(2), 168–185. https://doi.org/10.1108/AJAR-12-2023-0413

Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024). Cyber Risk Management Disclosure: *IJEBD (International Journal of Entrepreneurship and Business Development)*, *7*(5), 929–937. https://doi.org/10.29138/ijebd.v7i5.2844

Susanto, & Soepriyanto, G. (2024). Cybersecurity disclosure and audit fees: An empirical study of listed companies on the Indonesia stock exchange. *Edelweiss Applied Science and Technology*, *8*(6), 6090–6104. https://doi.org/10.55214/25768484.v8i6.3328

Telkom Indonesia (2020). Laporan Tahunan 2020. *PT Telkom Indonesia (Persero) Tbk.* https://www.telkom.co.id/sites/hubungan-investor/id_ID/page/laporan-1025

Telkom Indonesia (2021). Laporan Tahunan 2021. *PT Telkom Indonesia (Persero) Tbk.* https://www.telkom.co.id/sites/hubungan-investor/id_ID/page/laporan-1025

Telkom Indonesia (2022). Laporan Tahunan 2022. *PT Telkom Indonesia (Persero) Tbk.* https://www.telkom.co.id/sites/hubungan-investor/id_ID/page/laporan-1025

Telkom Indonesia (2023). Laporan Tahunan 2023. *PT Telkom Indonesia (Persero) Tbk.* https://www.telkom.co.id/sites/hubungan-investor/id_ID/page/laporan-1025

Telkom Indonesia (2024). Laporan Tahunan 2024. *PT Telkom Indonesia (Persero) Tbk.* https://www.telkom.co.id/sites/hubungan-investor/id_ID/page/laporan-1025

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*.